IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Robert GOLD

Serial No.: 09/832,067

Filed: April 9, 2001

For: METHOD AND SYSTEM FOR SYNCHRONIZING AND SELECTIVELY ADDRESSING MULTIPLE RECEIVERS IN A WIRELESS, SPREAD SPECTRUM COMMUNICATION SYSTEM

Customer No.: 29000

Confirmation No.: 1097

Group Art Unit: 3662

Examiner: Gregory, Bernarr E.

13/164

PETITION FOR RESCISSION OF SECRECY ORDER PURSUANT TO 37 C.F.R. § 5.4 and MPEP § 120

Commissioner for Patents
Office of Licensing and Review
Mail Stop L&R
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Assignee of the instant patent application is Robert Gold Communication Systems, Inc. ("RGCS"). RGCS hereby petitions for the rescission of the Secrecy Order imposed in connection with this application, on the ground that the subject matter of the application has been published jointly with the applicable defense agency (the United States Air Force) and has also been approved for further publication by the same agency. Thus, the Secrecy Order has become futile or

CERTIFICATE OF MAILING
(37 C.F.R. §1.8a)

I hereby certify that this paper (along with any referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

November 13, 2006
Date of Deposit

Connie Kwon
Connie Kwon

ineffectual, and its purpose is no longer being served. Moreover, its continuing existence will hinder commercialization of the invention.

This petition is submitted in duplicate as required by 37 CFR 5.4(a).

It is believed that no fee is required for this submission. However, if Applicant is incorrect in this regard, the Commissioner is hereby authorized to charge any fees which may be required to Deposit Account No. **09-0946**.

REMARKS

The invention was originally developed by RGCS for the United States Air Force, specifically the Air Force Research Laboratory of Wright-Patterson Air Force Base, under government contract **F33615-01-C-1800**. The instant patent application for a "Method And System For Synchronizing And Selectively Addressing Multiple Receivers In A Wireless Spread Spectrum Communication System" was filed on April 9, 2001. A Type A secrecy order was imposed in February 2002 on the ground that publication might be detrimental to national security.

The patent application received allowance over four years ago, in July 2002, but has not been allowed to issue because the Secrecy Order has been annually renewed.

However, at various times in the past several years, the sponsoring agency (U.S. Air Force) approved and jointly authored various publications describing and explaining the invention. Given the fact that the invention has already been widely published over the course of the past several years, it is respectfully submitted that the Secrecy Order is no longer necessary and, as opposed to having a useful benefit, merely hinders the commercial exploitation of the invention.

The publications describing and explaining the invention, and jointly authored by and approved by the U.S. Air Force, include the following:

1. *"A Digital Simulation of a Self-Synchronizing Selective Addressing, Frequency Hopping Communication System"* - Cleared for public release 07 Dec 2001, ASC 01-2370.
2. *"New Technology Solves Security Issue in Wireless Communication"* - Cleared for public release 3 Apr 2003, SN-03-0156.
3. "*Gold Algorithms: New Technology Provides Security Protection in Wireless Communications*" published in the AFRL Horizons, Vol. 4, Number 3, Sep 2003, SN-03-02, http://www.afrlhorizons.com/Briefs/Sept03/SN0302.html.
4. "*Sensors Directorate Develops Countermeasures Against Frequency Agile Signals,*" an AFRL Success Story published in April 2002, 02-SN-05.

Copies of these items have been attached as Exhibits 1 through 4 hereto for convenience of the Office. The following derivative publications have been made available online:

5. "*Secure Comms Claimed with No Encryption,*" published in 1 Nov 2004 in EE Times Online, http://www.eetimes.com/article/showArticle.jhtml?articleId=51201605.
6. *"'Gold Codes' Developer Touts Wireless Security Scheme"* published online 21 Oct 2004 in CommsDesign, http://www.commsdesign.com/showArticle.jhtml?articleID=51000037.

Copies of these items have been attached as Exhibits 5 and 6 for convenience of the Office. The Air Force has also approved and/or jointly authored additional publications describing the invention, including *"Frequency Agile Signal Prediction"* (which was cleared for public release on February 29, 2000, ASC 99-2518).

These publications describe not only the basic function of the invention, but also its general concepts and implementation specifics. For example, the invention as set forth in allowed claim 1 is stated as follows:

> *1. A method for wireless communication, comprising the steps of:*
>
> *transmitting a series of transmissions at a predetermined frequency, said transmissions separated by one or more clock intervals pseudo-randomly determined according to an initial code word loaded into a transmitter feedback shift register;*
>
> *receiving said series of transmissions at a receiver;*
>
> *at said receiver, measuring relative times of arrival between consecutive ones of said transmissions;*
>
> *determining said initial code word in the transmitter feedback shift register from the measured relative times of arrival between the consecutive transmissions;*
>
> *matching a receiver feedback shift register to the initial code word, adjusted by an amount of time since receiving the first one of said consecutive transmissions; and*
>
> *using said receiver feedback shift register to carry out synchronized communication with the transmitter.*

The features of allowed claim 1 are described, for example, in the publications attached as Exhibits 1 and 2. The Exhibit 1 publication states:

"In a frequency hopped – code division multiple access system (FH-CDMA), the transmitter hops over a range of available frequencies in a pseudorandom (PN), yet deterministic, pattern. ... The receiver must stay synchronous as the transmitter hops over a range of frequencies many times per second." (Page 1)

"[RGCS] has developed new techniques for the synchronization of frequency hopping and other wide band communication systems. These techniques only require that the receiver monitor the relative times-of-arrival of one selected frequency (designated the Key frequency) of the many over which the transmitted signal hops. After measuring relatively few of these times-of-arrival the RGCS algorithm provides the receiver with the required information necessary for it to synchronize with the received signal.

* * *

In Figure 2 a model frequency hopper transmitter block diagram is presented [embodied as a tapped shift register]. The feedback taps and the Code-of-the-Day determines what the code sequence will be. The number of frequency taps into the binary [shift] register, determine how many frequencies the hopper can hop over.

* * *

The RGCS synchronization algorithm takes as its input the relative times-of-arrival of the selected Key frequency. Each transmission of the Key frequency is called a hit. The number of hits of the key frequency required by the algorithm

> *is N/M where N is the number of stages in the shift register and M is the number of shift register stages tapped for input to the frequency synthesizer.*
>
> *Using this new technique, the time required for synchronization of the frequency hopping communication link is made up of the time required to collect the data on the key frequencies plus the time required by the algorithm to compute the fill word [i.e., initial code word] necessary to synchronize the transmitter and the receiver." (Pages 2-3)*

Thus, Exhibit 1 describes the essentials of the basic invention as claimed. It includes a description of "transmitting a series of transmissions at a predetermined frequency" (i.e., the Key frequency) based on pseudo-random clock intervals (i.e., a "pseudorandom (PN), yet deterministic, pattern") according to an "initial code word" (i.e., fill word) loaded into a "transmitter shift register," "receiving" that series of transmissions "at a receiver," "measuring relative times of arrival" between consecutive transmissions, "determining said initial code word" (i.e., fill word) using the "measured relative times of arrival," "matching a receiver feedback shift register to the initial code word" (i.e., fill word), and then using the result "to carry out synchronized communication with the transmitter." All of these features are explained clearly in Exhibit 1.

The same basic principles of the invention are explained, for example, in the Exhibit 2 publication at pages 2-3:

> *"In a spread spectrum communications system, a transmission hops among numerous frequencies many times per second – for example, it might hop among 128 frequencies 1,024 times per second.*

> *When using the RGCS technology, each receiver is set to monitor one of these 128 frequencies. As a receiver detects "hits" or bursts of data on its frequency, the Gold Algorithm uses the time intervals between the hits to derive sync information. The output of the algorithm is used to synchronize the hopping pattern of the receiver with that of the transmitter, so normal communication can take place.*
>
> *The synchronization occurs automatically, without users having to enter passwords or take any action at all.*
>
> *Because the Gold Algorithm processes the sync information very rapidly, the hopping pattern can be changed very often during the course of a transmission. As a result, brute-force attacks aimed at decoding the hopping pattern would be pointless, since the pattern would have been changed long before a decoding effort could be successful."*

The Exhibit 3 publication also contains a similar description of the invention.

The publications not only describe the core technology, but also describe the various applications of it, including the aspects of selective addressing in a multiple-receiver environment. *See, e.g.*, Exhibit 1, page 3 (Section 4.0). While it is true that not every last detail of implementation appears in these articles, many such details can be derived from knowing the basic principles of the invention as set forth in the various publications listed previously.

In view of the widespread publication of the basic inventive principles, the Secrecy Order no long serves its purpose and should be rescinded for that reason alone. The Order should be rescinded as promptly as possible because it now has the effect of impeding beneficial commercial development and exploitation of the invention, and therefore severely impacts the Assignee's business.

The invention was developed under an SBIR contract which is intended to help foster small businesses, stimulate technological innovation, and commercialize technology with the assistance of federal funding. Unfortunately, with the Secrecy Order in place, Assignee is unable to bring the benefits of the invention to the commercial market.

As explained in more detail in the accompanying materials, the invention has many properties useful for ad hoc Wi-Fi radio networks, or for emergency radio (used by, e.g., police and firefighters) over virtual private networks. Among other things, receivers can be addressed individually or in selected groups, allowing the use of Internet Protocol broadcast and multicast methods; a receiver can enter and leave the network at any time; and a transmitter can determine the group membership. The last two factors are expected to be of particular interest in emerging voice-over-IP networks that span LANs and WANs.

While it is true that the Assignee may seek compensation at some point from the U.S. government for delays in allowing exploitation of the invention, the Assignee would prefer instead have the opportunity to further develop this technology in the commercial sector, where it would be greatly beneficial to the public and have many applications in wireless and cellular industries.

Assignee therefore respectfully urges the Office and/or responsible government agency to reconsider the need for the Secrecy Order in this case. Given that the basic principles of the invention have been jointly published over the course of several years with the approval and encouragement of the sponsoring agency (the U.S. Air Force), Assignee respectfully submits that the Secrecy Order should be rescinded, and that the useful commercialization of the invention thereby be permitted.

The undersigned has endeavored to provide all of the information need to decide the subject petition. However, if any additional information is required, the Office of Licensing and Review is invited to contact the undersigned by telephone to discuss those issues so that this petition may be granted at the earliest possible date.

Respectfully submitted,

IRELL & MANELLA LLP

Dated: November 13, 2006

By: Christopher A. Vanderlaan
Reg. No. 37,747

1800 Avenue of the Stars, Suite 900
Los Angeles, California 90067-4276
Telephone: (310) 277-1010

EXHIBIT 1

Serial No. 09/832,067

Applicant: Robert Gold

A Digital Simulation of a Self-Synchronizing, Selective Addressing, Frequency Hopping Communication System

James P. Stephens, Sr.
Air Force Research Laboratory
Sensors Directorate
Wright-Patterson AFB, OH

Robert Gold, Ph.D.
Robert Gold Comm Systems Inc.
Los Angeles, CA

Abstract

This paper describes research and development activities for the implementation of a self-synchronizing, selective addressing, frequency hopping communication system. The algorithms used to implement this system are the result of work by Dr. Robert Gold, president of Robert Gold Communication Systems (RGCS), Inc., Los Angeles, CA. The algorithms are based on, Dr. Gold's technique for using 'times-of-arrival' of a few transmissions on a single frequency to determine the hopping pattern of frequency agile signals. Some potential commercial applications of this algorithm are provided.

1.0 Introduction

The development of techniques for the rapid achievement of synchronization is one of the most important and challenging tasks in the design of frequency hopping systems. Current solutions to this problem may involve sending synchronization information to the receiver by means of an auxiliary channel or by sending the information necessary to synchronize transmitter and receiver in some non frequency-hopping format. These fixes to the synchronization problem tend to degrade system performance with respect to its privacy and multiplexing capabilities.

This paper describes new research of a self-synchronizing, selective addressing, frequency hopping communication system. The work is based on using 'times-of-arrival' of a few transmissions on a single frequency to determine the hopping pattern of frequency agile signals. The use of this technique for cooperative frequency agile signals allows system synchronization to be achieved in milliseconds A cooperative system is one in which the frequency hopping parameters are known, in fact, the system is designed in such a manner to take advantage of this algorithm to improve its performance

2.0 Frequency Hopping Communication Systems

Frequency hopping spread spectrum modulation techniques in the past were used exclusively for military applications to minimize the effectiveness of electronic countermeasures. In recent years, frequency hopping is being used commercially to provide improved privacy, decreased narrowband interference, and increased signal capacity. In a frequency hopped – code division multiple access system (FH-CDMA), the transmitter hops over a range of available frequencies in a pseudorandom (PN), yet deterministic, pattern. The receiver must operate in synchronization with the transmitter, such that they are tuned to the same center frequency at the same time. A short burst of data is transmitted, usually by narrowband frequency shift keying (FSK) during each center frequency dwell time. Then, the transmitter tunes to another center frequency and transmits again. The receiver must stay synchronous as the transmitter hops over a range of frequencies many times per second. In a networked system, different communication links will have different hopping patterns, thus providing the capability for many distinct communication links to operate simultaneously in the same environment without interfering with one another (CDMA). RGCS's time-difference-of-arrival (TDOA) technique that is the focus of this paper offers improved synchronization performance and a selective addressing scheme for such a system. This is because the RGCS algorithm requires the receiver to monitor only a single frequency among the many that the transmitter may hop over. The receiver collects a relatively small number of relative-times-of-arrivals of the monitored frequency, and the algorithm determines the present state of the transmitter code generator, thereby obtaining synchronization. Selective addressing is achieved by not transmitting on the monitor frequency of the receivers that you do not wish to communicate with.

3.0 The RGCS Synchronization Algorithm

Robert Gold Comm Systems, Inc. (RGCS) under Air Force Contract F33615-01-C-1800 has developed new techniques for the synchronization of frequency hopping and other wide band communication systems. These techniques only require that the receiver monitor the relative times-of-arrival of one selected frequency (designated the Key Frequency) of the many over which the transmitted signal hops. After measuring relatively few of these times-of-arrival the RGCS algorithm provides the receiver with the required information necessary for it to synchronize with the received signal. Figure 1 provides a top-level description of the synchronization process.

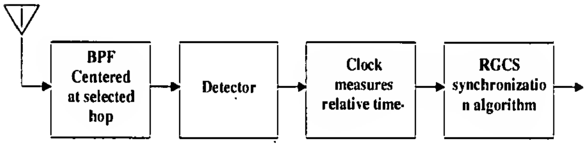

BPF Centered at selected hop
Detector
Clock measures relative time·
RGCS synchronizatio n algorithm

Figure 1 - RGCS Synchronization Technique

In Figure 2 a model frequency hopper transmitter block diagram is presented. The feedback taps and the Code-of-the-Day (COD) determines what the code sequence will be. The number of frequency taps into the binary register, determine how many frequencies the hopper can hop over. That is, if the binary register has M stages then the hopper can hop over 2^M frequencies. The combination of the frequency taps placement and the frequency mapper determine what specific frequencies the radio will hop among. In a cooperative system, the RGCS algorithm has knowledge of all these parameters.

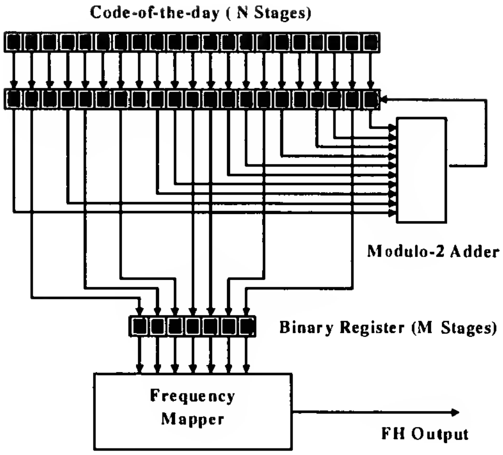


Figure 2 – Model Frequency Hopper

3.1 Algorithm Performance

The RGCS synchronization algorithm takes as its input, the relative times-of-arrival of the selected Key Frequency. Each transmission of the Key Frequency is called a hit. The number of hits of the key frequency required by the algorithm is $\frac{N}{M}$ where N is the number of stages in the shift register and M is the number of shift register stages tapped for input to the frequency synthesizer.

Using this new technique, the time required for synchronization of the frequency hopping communication link is made up of the time required to collect the data on the key frequencies plus the time required by the algorithm to compute the fill word necessary to synchronize the transmitter and the receiver. Of these two times, the former is the most significant. For example, if the hopper is hopping over 128 frequencies ($M = 7$) at a rate of 1024 hops per second, then the receiver will, on the average, receive Key Frequencies at a rate of 1024/128 = 8 hops per second. If the hopper shift register has 16 stages ($N = 16$) then the time to collect the required $\frac{N}{M} = \frac{16}{7} \approx 3$ Key frequencies is .375 seconds.

The performance of the RGCS synchronization algorithm is highly dependent upon the setting of the receiver threshold for determining the reception of a hit. The setting of this threshold is a trade-off between probability of synchronization failure and time to synchronize. Since the RGCS synchronization algorithm can tolerate missed hits but fails catastrophically when presented with a false hit, this suggests setting the hit threshold as high as possible to prevent the acceptance of false hits and reduce the probability of synchronization failure. However, setting the hit threshold high will cause some valid hits to be missed thereby increasing the expected time required to collect the number of hits needed by the algorithm. The proper setting for the hit threshold is critical for optimal performance.

Figure 3 is a plot of the expected time to synchronize vs the threshold to noise ratio for a hopper over 128 frequencies using a 16-stage shift register. It shows that at optimum receiver threshold setting at 13db S/N ratio the expected time to synchronize is 1.2 seconds..

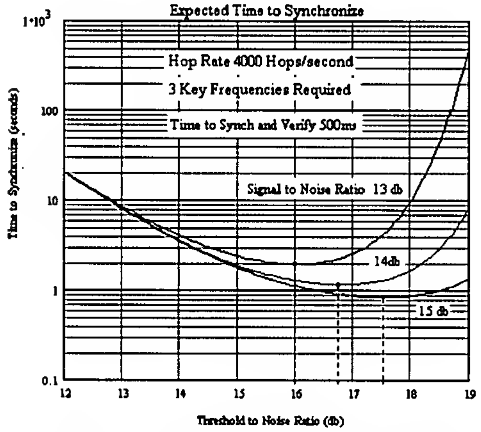


Figure 3 Expected Time to Synchronize (500ms)

4.0 Multiplexing and Selective Addressing

The technique also provides for multiplexing and unique addressing capabilities. The synchronization, multiplexing and addressing capability achieved by the RGCS technique may be explained by reference to Figure 4. The transmitter frequency-hopping pattern dictates that the transmitter hop over all the frequency slots F_1 through F_n. A selected set of frequencies S_1 through S_k is assigned as synchronization frequencies and the transmitter is disabled when the frequency-hopping pattern dictates that one of these synchronization frequencies is to be transmitted. Each receiver of the communications net is assigned a unique synchronization frequency. When a transmitter wants to address a receiver or a set of receivers he enables the synchronization frequency that was assigned to those receivers and each receiver can use the times of arrival to obtain the necessary synchronization information required to receive the hopped signal.

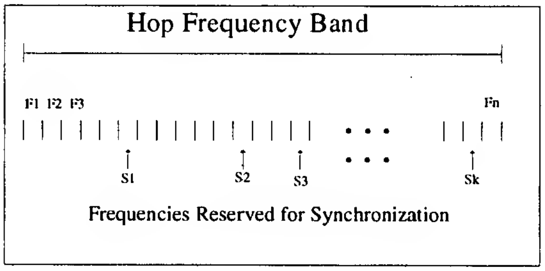


Figure 4 - Multiplexing and Addressing Capability

5.0 Hardware Demonstration System

This section contains the functional requirements for a hardware system to demonstrate the RGCS synchronization algorithm. The demonstration system consists of multiple PCs, one serving as the transmitter and the others the receivers of a one-way encrypted audio link. The use of multiple receivers allows for the demonstration of selective addressing and simultaneous aural comparison of the decoded and coded audio signals. The data path is a cable interconnecting the serial (i.e., RS-232) ports of the transmitter PC with the receiver PCs.

The basic system is shown in Figure 5. Note that only one receiver is required, with an optional second receiver required only for demonstrating selective addressing and for simultaneous comparison between the coded and decoded audio output signals. A top-level block diagram of the system is shown in Figure 6. Test carried out using this demonstration systems have shown that the algorithm is capable of synchronizing frequency hopping communication systems in under 500ms.

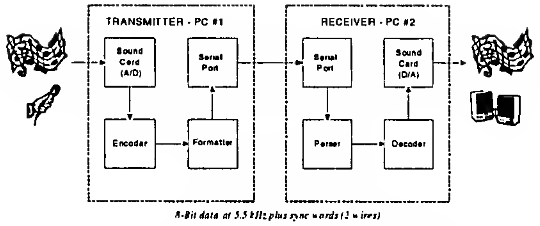


Figure 5 - Basic Demonstration System

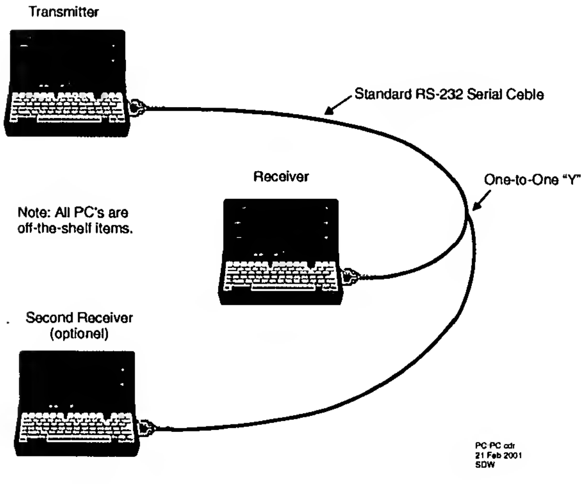

Transmitter
Standard RS-232 Serial Cable
Receiver
One-to-One "Y"
Note: All PC's are off-the-shelf items.
Second Receiver (optional)
PC-PC cdr
21 Feb 2001
SDW

Figure 6 - Top-Level Block Diagram

6.0 Summary

The Federal Communication Commission (FCC) amended rules in 1985 to allow commercial frequency hopping spread spectrum in the Industrial, Medical, and Scientific (ISM) 2.4 GHz band (Part 15). The rule change was designed to foster development of wireless local area networks (LAN) and wireless cable modems, thus enabling wider bandwidths that will allow Internet devices to operate at higher speeds. The wireless LAN standard IEEE 802.11 specifies frequency hopping in the ISM band of 2.400 to 2.483 GHz in a series of 1 MHz channels up to 79 separate and distinct channels. Bluetooth is another wireless technology that plans to provide standards that will replace cables. The Bluetooth standard provides for small, inexpensive chips that can be integrated into computers, printers, mobile phones, etc. to replace cables by taking information normally carried by the cable and transmitting it over a short distance RF link. Although not always utilized, most commercial cellular radio systems such as GSM (Groupe Spécial Mobile) and the newer 3GPP^{TM} (3rd Generation Partnership Project) have frequency hopping capabilities written into their specifications. The processes described by this paper are applicable to many of these proposed commercial applications.

References

1. Stephens Sr., James P. and Robert Gold, "Frequency Agile Signal Prediction", Proceedings of Threats, Countermeasures, and Situational Awareness – Teaming for Survivability, June 20-22, 2000, Virginia Beach, VA.

Biographies

James P. Stephens

Since January 1991, Mr. Stephens has been employed as an electronics engineer with the Air Force Research Laboratory, Sensors Directorate, RF Sensor Technology Division, Electronic Warfare Technology Branch, at Wright-Patterson Air Force Base, Ohio. He is responsible for the planning and execution of research projects which will exploit the theory of communications jamming concepts applicable to future Air Force needs and objectives. His research activities involve both in-house and contractual efforts in communications countermeasures toward the development and evaluation of concepts, systems, and supporting technologies with emphasis on spread spectrum, low probability-of-intercept (LPI) waveforms, and digital signal processing techniques. Mr. Stephens was previously assigned to National Air Intelligence Center (NAIC, formerly Foreign Technology Division), Directorate of Technology and Threat, as an electronics engineering analyst from 1982 to 1991. He was also employed by the Federal Communication Commission from 1969 to 1982. Mr. Stephens received an MSEE from the Air Force Institute of Technology in 1990 and a BSEE from West Virginia Institute of Technology in 1969.

Dr. Robert Gold

Dr. Robert Gold has over 34 years of heavy involvement in the research, development, and design of signals for electronic warfare applications. He has developed unique capabilities in, and made major contributions to the theory, design, and analysis of coded communication systems, which have made him internationally recognized authority in this field. In 1967, Dr. Gold founded Robert Gold Associates which has established a record of successful accomplishments in the fields of covert communications, coding theory, mathematical modeling, operations research, and spread spectrum communication systems. He has directed the company in a series of contractual studies which have supplied crucial support to a number of military communication systems. As Manager of Mathematical Analysis at Magnavox Research Laboratories, Torrance CA from 1961 to 1967, he was project leader for research studies concerned with the determination of the properties of pseudo random binary encoding sequences and their application to spread spectrum, low probability-of-intercept (LPI) radar, and other secure communication systems. As Technical Director and Director of Research from 1983 to 1987 for the Electronic Warfare Laboratory of Gould, Inc., El Monte CA, Dr. Gold has had administrative, marketing and technical responsibility for research and development programs concerning ECM, ECCM, and ESM systems. Dr. Gold's achievements include code design for the Navy FLEETSATCOM, the Air Force Global Positioning System (GPS), and the NASA Tracking and Data Relay Satellite System (TDRSS). He has also performed significant work in the areas of IFF coding, including the NATO Identification System as well as frequency hopping techniques and covert signal processing. Dr. Gold has authored many classified and unclassified publications in the field of coded communications and many of his contributions have resulted in significant improvements in system performance. He is perhaps best known for his invention of "Gold Codes."

EXHIBIT 2

Serial No. 09/832,067

Applicant: Robert Gold

New Technology Solves Security Issue In Wireless Communications

Los Angeles – New technology that provides powerful security protection for wireless computer networks, cell phones and other radio communications has been developed by Robert Gold Comm Systems.

The company is headed by Dr. Robert Gold, an internationally known expert in coding algorithms and developer of the Gold Codes used in the Global Positioning System (GPS) network. Dr. Gold also oversaw signal design for NASA's satellite-based tracking and data relay systems.

The new Gold Algorithm was developed under contract to the U.S. Air Force. It is designed to be integrated into the spread spectrum or frequency hopping systems widely used for wireless communications, such as "Wi-Fi" computer networks, cellular phones and two-way radios used by the military, police, firefighters, ambulances and commercial fleets.

THE PROBLEM

Although very convenient for users, wireless communication is extremely vulnerable to eavesdropping. Wireless computer networks, for example, are frequently accessed by hackers or even innocent bypassers whose laptop computers link up with the network.

The security of these networks can be increased by encrypting the data, but encryption is complex, inconvenient and time-consuming for users, and adds a significant amount of overhead information that reduces data throughput.

In spread spectrum or frequency hopping networks now in wide use, data is protected by rapidly changing the frequency over which the transmission is sent, among the hundreds of frequencies over which the transmitter hops. The pattern of these changes, which can occur hundreds or thousands of times per second, must be known by a receiver in order for it to synchronize to the hopping pattern of the transmitter and establish communication. An intruder without knowledge of the synchronization pattern would not be able to intercept the communication, and may not even be aware communication is taking place.

However, spread spectrum networks have a major vulnerability. Information about this sync pattern must be sent to authorized receivers. Often sync information is based on an external clock or other information that must be communicated "in the clear," or unprotected. If an intruder intercepts this information, the security of the network is compromised.

THE RGCS SOLUTION

Robert Gold Comm Systems has developed a breakthrough self-synchronizing technique that provides secure messaging in wireless communications system. The patented technology, available for licensing, permits transmitters and receivers in a spread spectrum environment

to rapidly and automatically synchronize their frequency hopping patterns without the need for external clocks or for "in the clear" transmission of the sync information.
Benefits of the Gold Algorithm include:

- Highly **secure communication** without the overhead of encryption
- Selective **addressability of receivers**, individually or in groups, so receivers on the network can instantly be included or excluded for specific messages
- Highly **efficient utilization of bandwidth**
- **Immediate access** (no dialup or connect delay)
- Random access; receivers can **enter the network at any time**
- **Resistance to interference**

The RGCS technology offers important competitive advantages to manufacturers of wireless local area computer networks (WLANs), including Wi-Fi installations and virtual private networks (VPNs); cell phones; military, police and civilian radio systems; satellite TV networks; voice over Internet protocol (VOIP) systems and other technologies that require secure, efficient use of broadcast spectrum.

The Gold Algorithm is designed to be incorporated into enhanced versions of existing products, many of which already include circuitry that can be adapted to implement the technology. (For this reason, RGCS has no plans to manufacture its own chips incorporating the algorithm.)

HOW THE TECHNOLOGY WORKS

In a spread spectrum communications system, a transmission hops among numerous frequencies many times per second – for example, it might hop among 128 frequencies 1,024 times per second.

When using the RGCS technology, each receiver is set to monitor one of these 128 frequencies. As a receiver detects "hits" or bursts of data on its frequency, the Gold Algorithm uses the time intervals between the hits to derive sync information. The output of the algorithm is used to synchronize the hopping pattern of the receiver with that of the transmitter, so normal communication can take place.

The synchronization occurs automatically, without users having to enter passwords or take any action at all.

Because the Gold Algorithm processes the sync information very rapidly, the hopping pattern can be changed very often during the course of a transmission. As a result, brute-force attacks aimed at decoding the hopping pattern would be pointless, since the pattern would have been changed long before a decoding effort could be successful.

Communication to each receiver is enabled or blocked simply by switching on or off the transmission of signals on the frequency the receiver monitors. This enables users to create networks that are both secure and very flexible.

In a police department's radio network, for example, a dispatcher could communicate privately with one patrol car without distracting other officers from their activities. At a crime scene, officers could instantly create an ad hoc network that would include those at the scene and selected supervisors at headquarters, and would exclude officers busy with other duties.

The Gold Algorithm supports CDMA (code-division multiple access), FMHA (frequency hopping multiple access) and UWB (ultra wide band) spread spectrum communication systems.

APPLICATIONS OF RGCS TECHNOLOGY

Potential applications of the Gold Algorithm include highly secure versions of wireless computer networks; cell phones; dispatch radio communications for police, ambulance and commercial purposes; military field radios; covert agent and downed pilot communications; "smart" broadcast and satellite delivery of video, audio and data with real-time authorization of receivers; control of remotely piloted vehicles and other devices, among other uses. "This technology offers important advantages to manufacturers of a wide range of products, and important benefits to the users of those products," said Dr. Gold.

"As a software-based solution, it provides manufacturers with very significant performance improvements and product differentiation without requiring major redesign of existing products. For the users of these products, benefits include always-on robust security, without the need for passwords or indeed any other intervention by the user."

ABOUT ROBERT GOLD COMM SYSTEMS

Robert Gold Comm Systems, Inc., was founded to develop and commercialize a self-synchronizing technology to provide security and increased functionality for spread spectrum communications. The company, located in Los Angeles, is headed by Dr. Robert Gold, who for more than 30 years has made major contributions to the theory, design, and analysis of coded communication systems, and is an internationally recognized authority in this field.

Dr. Gold's achievements include code design for the Air Force Global Positioning System (GPS), the NASA Tracking and Data Relay Satellite System (TDRSS) and the Navy FLEETSATCOM. He has authored many classified and unclassified publications in the field of coded communications. He is perhaps best known for his invention of the "Gold Codes."

# # #

Note to editors: Click here to view a Powerpoint presentation on the RGCS technology

Press contact:

Alexander Auerbach
Auerbach & Co., Inc.
1-800-871-2583
auerbach@aapr.com

EXHIBIT 3

Serial No. 09/832,067

Applicant: Robert Gold

Gold Algorithms

New technology provides security protection in wireless communications.

AFRL's Sensors Directorate, Radio Frequency Sensor Division, Electronic Warfare Technology Branch, Wright-Patterson AFB OH

Robert Gold Comm Systems (RGCS), Inc. developed new technology that provides powerful security protection for wireless computer networks, cell phones, and other radio communications. The company is headed by Dr. Robert Gold, an internationally known expert in coding algorithms and developer of the Gold Codes used in the Global Positioning System network. Dr. Gold also oversaw signal design for the National Aeronautics and Space Administration's Tracking and Data Relay Satellite System (known as TDRSS).

RGCS developed the new Gold Algorithms under contract to the US Air Force. RGCS designed the algorithms for integration into the spread-spectrum or frequency-hopping systems widely used for wireless communications such as wireless fidelity (commonly known as Wi-Fi) computer networks; cellular phones; and two-way radios used by the military, police, firefighters, ambulances, and commercial fleets.

Although very convenient for users, wireless communication is extremely vulnerable to eavesdropping. For example, hackers frequently access wireless computer networks (laptop computers linking to the network). Encrypting the data increases the security of these networks, but encryption is complex, inconvenient, and time-consuming for users, and it adds a significant amount of overhead information that reduces data throughput.

In the spread-spectrum or frequency-hopping networks now in wide use, data is protected by sending it in brief spurts, with the transmitter and receiver skipping in a synchronized pattern among hundreds of frequencies. An intruder without knowledge of the synchronization pattern would just hear static. However, many spread-spectrum networks have a major vulnerability. The originator must send the sync pattern information to authorized receivers. Often this sync information is communicated "in the clear," or unprotected. If an intruder intercepts this information, the security of the network is compromised.

RGCS developed a breakthrough, self-synchronizing technique that provides secure messaging in wireless communication systems. The patented technology, available for licensing, permits transmitters and receivers in a spread-spectrum environment to rapidly and automatically synchronize their frequency-hopping patterns without the need for external or in-the-clear transmission of the sync information. Benefits of the Gold Algorithms include highly secure communication without the overhead of encryption; selective addressability of receivers, individually or in groups, so receivers on the network can instantly be included or excluded for specific messages; highly efficient utilization of bandwidth; immediate access (no dial-up or connect delay); random access (receivers can enter the network at any time); and resistance to interference.

In a frequency-hopping, spread-spectrum communications system, a transmission hops among numerous frequencies many times per second (e.g., it might hop among 128 frequencies 1,024 times per second). When using the RGCS technology, the user sets each receiver to monitor one of these frequencies. As a receiver detects bursts of energy on its frequency, the Gold Algorithms calculate the time intervals between them. The output of the algorithms synchronizes the hopping pattern of the receiver with that of the transmitter, so normal communication can take place. The synchronization occurs automatically without users having to enter passwords or take any action at all.

Because the Gold Algorithms process the sync information very rapidly, the user can change the hopping pattern phase very often during the course of a transmission. As a result, brute-force attacks aimed at decoding the hopping pattern are pointless, since the pattern would have changed long before a decoding effort could be successful.

To enable or block receiver communication, the sender simply switches the signals transmission, on the frequency the receiver monitors, to "on" or "off". This enables users to create networks that are both secure and very flexible. In a police department's radio network, for example, a dispatcher could communicate privately with one patrol car without distracting other officers. At a crime scene, officers could instantly create an ad hoc network that would include those at the scene and selected supervisors at headquarters, excluding officers busy with other duties.

The Gold Algorithms support code-division multiple access; frequency-hopping multiple access; and ultra-wide-band, spread-spectrum communication systems. Potential applications of the Gold Algorithms include highly secure versions of wireless computer networks; cell phones; dispatch radio communications for police, ambulance, and commercial purposes; military field radios; covert agent and downed pilot communications; smart broadcast and satellite delivery of video, audio, and data with real-time authorization receivers; control of remotely piloted vehicles; and other devices.

RGCS designed the Gold Algorithms for

incorporation into enhanced versions of existing products, most of which already include circuitry that manufacturers can adapt to implement the technology. "This technology offers important advantages to manufacturers of a wide range of products and important benefits to the users of those products," said Dr. Gold. "As a software-based solution, it provides manufacturers with very significant performance improvements and product differentiation without requiring major redesign of existing products. For the users of these products, benefits include always-on robust security without the need for passwords or indeed any other intervention by the user."

Mr. James Stephens and Dr. Robert Gold (Robert Gold Comm Systems, Inc.), of the Air Force Research Laboratory's Sensors Directorate*, wrote this article. For more information contact TECH CONNECT at (800) 203-6451 or place a request at* http://www.afrl.af.mil/techconn/index.htm. *Reference document SN-03-02.*

DISTRIBUTION A
PUBLIC RELEASE

HOME | ABOUT AFRL | CONTACT US | DISCLAIMER

EXHIBIT 4

Serial No. 09/832,067

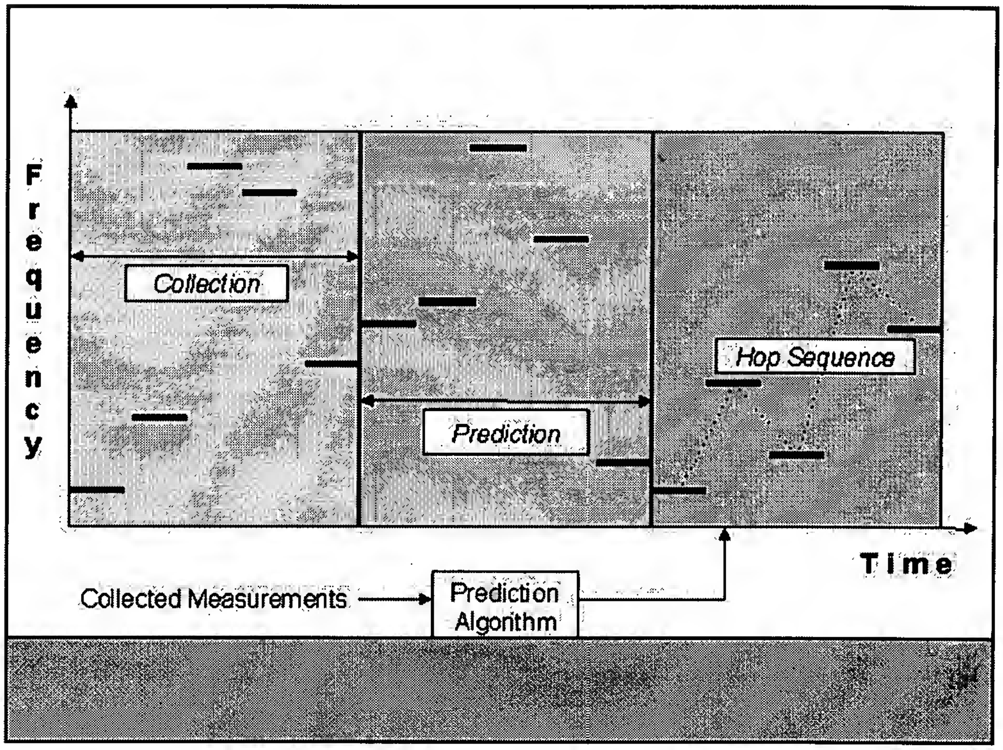
Applicant: Robert Gold

Air Force Research Laboratory | AFRL

Science and Technology for Tomorrow's Aerospace Forces

Success Story

SENSORS DIRECTORATE DEVELOPS COUNTERMEASURES AGAINST FREQUENCY AGILE SIGNALS



The Sensors Directorate's successful software implementation of the hop prediction system provides a valuable baseline to the hardware implementation of the frequency agile prediction system. The time-difference-of-arrival technique will provide increased capability, particularly against fast frequency hoppers, at lower cost and complexity of hardware since it monitors only one frequency among the many the system can hop over.

Air Force Research Laboratory
Wright-Patterson AFB OH

Sensors
Emerging Technologies

Accomplishment

In a joint effort with Robert Gold Communication Systems (RGCS), directorate scientists are developing countermeasures against frequency agile signals. Engineers use frequency agile signals to provide resistance to jamming, reduce the likelihood against detection, and offer protection from enemy missiles.

RGCS engineers developed software that uses the time-of-arrival of a few transmissions to determine the hopping pattern of frequency agile signals. As hop rates and standoff distances increase, propagation distances and processing time make it impossible to use "follower" jamming techniques to combat frequency agile signals. Scientists can overcome this deficiency by using times-of-arrival processing techniques.

Background

While two aircraft are communicating over a relatively short range, a standoff sensor or jammer must receive the signal, process the signal, and transmit a jamming signal back to the receiver. The aircraft must complete this process before the receiver changes to another frequency in response to the frequency agility of the target transmitter. As technology continues to develop, frequency synthesizers, used in frequency hopping spread spectrum communication and radar systems, will operate at increasingly higher hop rates, and repeat-back or frequency-follower jammers will become less effective.

Since engineers developed frequency synthesizer implementations that operate at several hundred thousand hops per second and since rates in excess of one million hops per second are entirely feasible, the futility of pursing a follower jammer is clear. Tactical airborne military electronic attack and electronic protection systems have the requirement that any technique developed must operate in real time. This requirement is due to the rapidly changing nature of the battle scenario, the typically short message bursts, and the ability of the uncooperative target link to change the code-of-the-day.

Directorate researchers studied algorithmic techniques to identify information concerning the hard-wired and logical structure of the hopper equipment used by the algorithm to exploit these weaknesses. The time-difference-of-arrival technique requires a collection time where times-of-arrival to single frequency are made. Then the algorithm goes to work, determines the sequence, achieves synchronization, and predicts where and when each successive frequency occurs.

Additional information

To receive more information about this or other activities in the Air Force Research Laboratory, contact TECH CONNECT, AFRL/XPTC, (800) 203-6451 and you will be directed to the appropriate laboratory expert. (02-SN-05)

EXHIBIT 5

Serial No. 09/832,067

Applicant: Robert Gold

CMP
United Business Media
EETIMES ONLINE

EE Times:

Secure comms claimed with no encryption

Loring Wirbel

(11/01/2004 10:00 AM EST)
.URL: http://www.eetimes.com/showArticle.jhtml?articleID=51201605

Colorado Springs, Colo. — The developer of the eponymous "Gold codes" has demonstrated a self-synchronized receiver technology that he says will enhance security in wireless LANs, cellular networks and ultrawideband systems. Robert Gold's company, Robert Gold Comm Systems Inc. (Carlsbad, Calif.), has demonstrated a two-receiver system to the U.S. Air Force, and is licensing its software code to semiconductor manufacturers.

Gold is well-known in RF and DSP algorithm circles for his work in the 1980s on an algorithm that uses sequences of pseudorandom numbers that can be generated with two feedback shift registers. These "Gold codes" provide autocorrelation and cross-correlation for wireless networks and have been used within in-building wireless radio networks, UMTS digital cellular networks and the GPS satellite system.

Gold's current work stemmed from an Air Force basic-research contract to explore ways to improve the security of all spread-spectrum systems, whether direct-sequence or frequency hopping. Gold said he has developed an efficient module of embedded software for transmitters and receivers that allows them to synchronize their patterns in milliseconds without the use of external clocks. Software for the self-synchronizer occupies only 7,000 lines of code in a Windows environment, and can be made even more compact when compiled for embedded environments.

"It represents very little overhead, even in constrained environments like handsets," Gold said.

Internet orientation
Gold's company completed a study under the Air Force's Small Business Innovative Research program that led to delivery of a two-receiver frequency-hopping test bed. The contract was conducted under the RF sensor division of the Electronic Warfare Technology Branch at Wright-Patterson Air Force Base in Ohio.

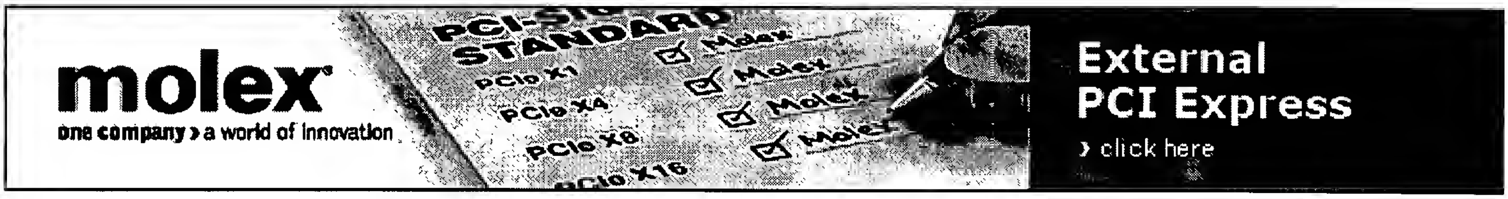
The algorithm has several properties useful for ad hoc Wi-Fi radio networks and police/fire radio using virtual private networks: Communications can be secure without the use of encryption; receivers can be addressed individually or in selected groups, allowing the use of Internet Protocol broadcast and multicast methods; a receiver can enter and leave the network at any time; and a transmitter will securely confirm group membership. The last two factors could be of particular interest in emerging voice-over-IP networks that span LANs and WANs, Gold said.

While the Air Force is exploring a range of open and classified applications for the technology, Gold's company (www.rgcsystems.com) is free to license the basic algorithms for commercial applications.

EXHIBIT 6

Serial No. 09/832,067

Applicant: Robert Gold



CommsDesign

'Gold codes' developer touts wireless security scheme

Loring Wirbel
Oct 21, 2004 (1:45 PM)
URL: http://www.commsdesign.com/showArticle.jhtml?articleID=51000037

COLORADO SPRINGS, Colo. — The developer of the pseudorandom "Gold codes" used in digital cellular networks and the Global Positioning System has demonstrated a self-synchronized receiver technology for enhancing security in wireless LANs, cellular networks and ultrawideband systems.

Robert Gold Comm Systems Inc. (Carlsbad, Calif.) has demonstrated a two-receiver system to the U.S..Air Force, and is licensing its software code to chip makers.

Gold is well known in the RF and DSP algorithm communities for his work in the 1980s on an algorithm that uses sequences of pseudorandom numbers easily generated with two feedback shift registers. The so-called "Gold codes" provide auto- and cross-correlation for wireless networks, and were used in early wireless radio networks and in the GPS satellite system.

The current work stems from a U.S. Air Force contract to explore ways of improving the security of spread-spectrum systems, including direct-sequence or frequency-hopping systems. In both types, information about the synchronization pattern used for spreading a signal must be sent to receivers in the clear, compromising basic system security.

Gold said he has proposed development of an efficient module of embedded software for transmitters and receivers that allow them to synchronize patterns without using external clocks. Network nodes can be synchronized in milliseconds, Gold said. Software for the self-synchronizer occupies only 7,000 lines of code in a Windows environment, and can compressed even more when compiled for embedded environments.

"It represents very little overhead, even in constrained environments like handsets," Gold said.

Gold's company completed a phase-one study under the Air Force's Small Business Innovative Research program, and has delivered a two-receiver frequency-hopping test bed to the Air Force. The contract was not related to a specific platform, Gold said, but was conducted as a basic research program under the RF sensor division of the Electronic Warfare Technology Branch at Wright-Patterson Air Force Base (Dayton, Ohio).

The algorithm has several properties useful for ad-hoc WiFi radio networks as well as for police and fire radios on virtual private networks. Secure communications are possible without using encryption, though the new receiver software can be used in conjunction with either private- or public-key encryption.

Receivers can be addressed individually or in selected groups, allowing the use of IP broadcast and multicast methods. A receiver also can enter and leave the network at any time, and a transmitter will securely confirm group membership. The last two factors could be of particular interest in emerging Voice-over-IP networks that span LANs and WANs, Gold said.

While the Air Force is exploring a range of and classified and unclassified applications for the technology, Gold's company is free to license the basic algorithms for commercial applications.

Gold said he has assembled a hardware and software implementation team, thereby making the startup more than a licensing clearinghouse. But Gold added that the company has no intention of moving directly into volume production of hardware systems.

Instead, the company will explore a range of licensing opportunities with OEMs, embedded software firms and chip manufacturers, though Gold said the software's most logical point for integration is at the single-chip level.

More information on terms is available at the company's Web site.